to one embodiment. Rendezvous peers cache peer and peer group information. Rendezvous access is restricted to peers with access privileges. Non-trusted peers contact local trusted peers to gain access. In one embodiment, the rendezvous policy may be used across subnets (configurable at peer group level). In one embodiment, the rendezvous policy may be used across/through firewalls (e.g. gateways). In one embodiment, the peer-to-peer platform may include a propagate policy. Figure 32 illustrates discovery through propagate proxies according to one embodiment. In one embodiment, the propagate policy may be used for subnet TCP/multicast (platform configurable). In one embodiment, the propagate policy may support HTTP gateways (platform configurable). In one embodiment, the propagate policy may be used through firewalls (e.g. need peer activation behind firewalls). Propagation is restricted to peers with access privileges. A discovery (propagate) proxy controls propagation through message counts and/or TTL (Time To Live) mechanisms. In one embodiment, the peer-to-peer platform may include an invite policy. In one embodiment, the invite policy may support the adding of new peers and peer groups (e.g. publish advertisements). In one embodiment, the peer-to-peer platform may allow the persistent local peer caching of discovery information.

A1 end

Please replace the paragraph beginning on line 12 of page 65 with:

Figures 19A through 19E illustrate embodiments of a peer-to-peer platform proxy service, and show various aspects of the operation of the proxy service. Figure 19A shows a firewall with an email gateway. A region with peers is shown inside the firewall, and another region with peers is shown outside the firewall. A proxy service is also shown outside the firewall. In one embodiment, the peer-to-peer platform proxy service may be used to bridge peer-to-peer platform protocols with HTTP, email and/or SOCKS as illustrated in Figure 19B. A proxy service may be used to enable peer group contact across firewalls. As illustrated in Figure 19C and 19D, the proxy service may allow peers to send requests to communicate across a firewall. Through the proxy service, peer-to-peer platform messages may be posted for delivery across the firewall. As

A2

A2 end illustrated in Figure 19E, in one embodiment, the proxy service may allow secure pipes to be established across firewalls as necessary.

Please replace the paragraph beginning on line 27 of page 66 with:

Figures 23 through 27 illustrate embodiments of peer group authentication in the peer-to-peer platform. Figure 23 illustrates several levels of login authentication that may be used according to one embodiment. These levels include anonymous login, plain text login (user or user plus password), and login with privacy, which uses public key exchange and symmetric master keys. The login process should return a credential to the logging-in peer. The peer uses the credential to bypass the login process until the credential expires. Figure 24 illustrates a peer-to-peer platform public key chain according to one embodiment. In this embodiment, a key chain for all registered peers is used to eliminate public key exchanges. This is unauthenticated access, and is open to "imposters in the middle" attacks. This is a first step towards a secure Public Key Infrastructure (PKI) with signed certificates.

A3

Please replace the paragraph beginning on line 10 of page 67 with:

Figure 26 illustrates integrity of data in a peer-to-peer platform according to one embodiment. A standard hash (SHA1) is used on data. Two forms of integrity, a weak form and a strong form, are illustrated. Other embodiments may utilize other integrity methods. The weak for uses a public key ring and symmetric master key to sign. The weak form uses a public key ring and symmetric master key to sign. The weak form works best between two peers each having the other's public key. The strong form uses asymmetric key algorithm such as RSA and Certificate Authorities. A peer-to-peer platform proxy Certificate Authority (CA) service creates, signs and distributes X509 certificates for all peers on a public key chain. A proxy service's public key must be resident on each proxied peer.

A4